Содержание

Введение

Этот документ описывает, как настроить сетевую Переадресацию (NAT) Трафик TCP распределения нагрузки сервера на маршрутизаторах iOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Цель

Пользователи, которые обращаются к локальному серверу из внешнего Интернета, обратятся к серверу с помощью одиночного URL или IP-адреса, однако устройство NAT используется для загрузки, совместно используют трафик пользователя ко множественным идентичным серверам с зеркальным содержанием.

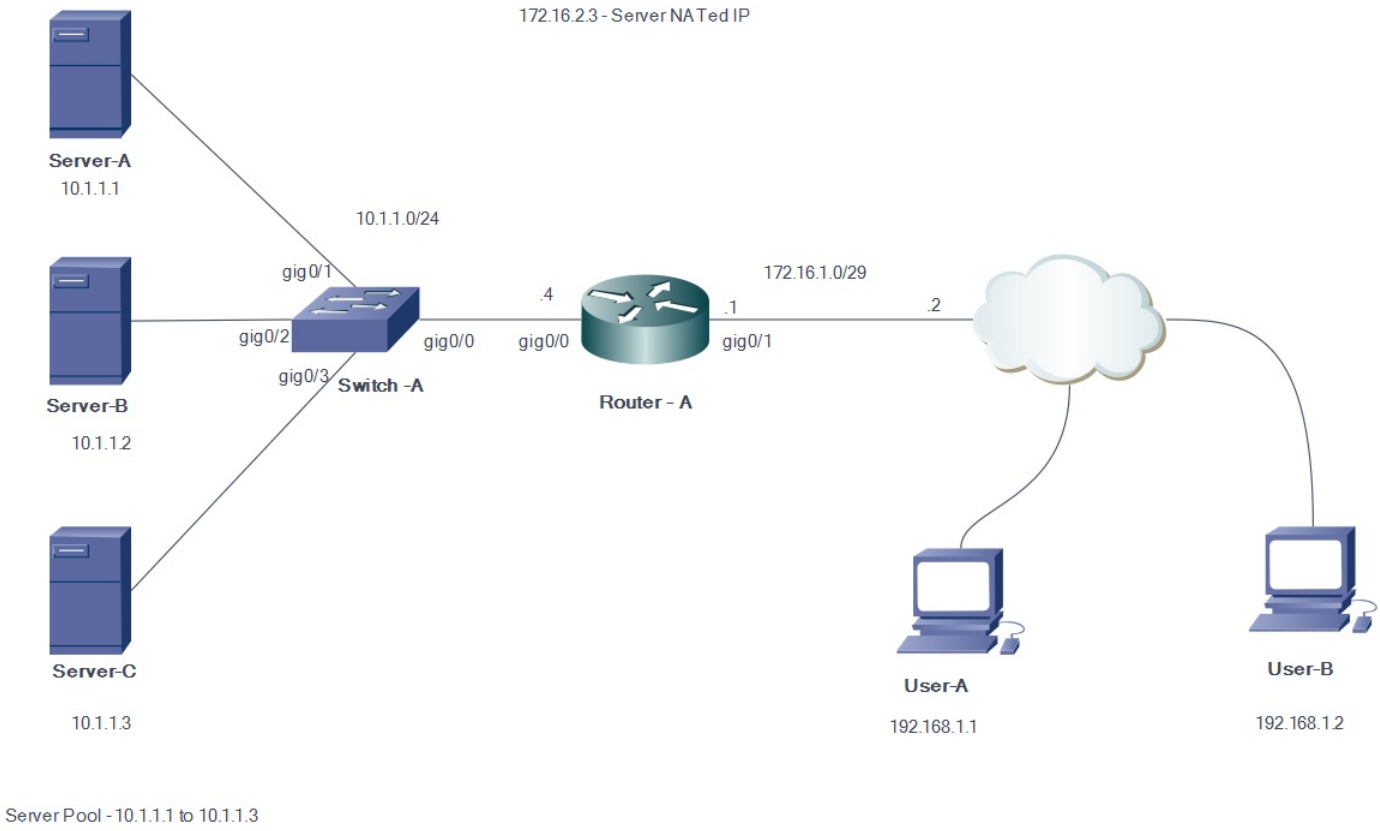
Описание

Внешние пользователи A и Б обращаются к содержанию Web-сервера с внешним видимым

IP 172.16.2.3 (Виртуальный IP из серверов). Маршрутизатор NAT преобразовывает их трафик, предназначенный для 172.16.2.3 к внутреннему IP? s 10.1.1.1, 10.1.1.2 и 10.1.1.3 в кольцевом способе обслуживания и вперед этом к соответствующему серверу. Каждый новый сеанс, инициируемый от внешнего пользователя, преобразован в следующий IP-адрес физического сервера.

Настройка

Схема сети



Шаги

1. Здесь Усера инициирует TCP - подключение с ip виртуального сервера 172.16.2.3
2. Маршрутизатор NAT после получения запроса подключения, создает запись преобразования NAT, выделяя следующий доступный IP-адрес реального сервера (например, 10.1.1.1).
3. Маршрутизатор NAT заменяет IP - адрес назначения выделенным реальным IP - адресом и передает пакет.
4. Сервер получает пакет и отвечает назад на источник.
5. Маршрутизатор NAT получает пакет, возвратился из сервера и выполняет поиск таблиц NAT. Маршрутизатор тогда преобразовывает адрес источника в IP-адрес виртуального сервера (172.16.2.3) и передает пакет.
6. Теперь пользователь-B инициирует сеанс TCP с сервером виртуальные IP 172.16.2.3, теперь после получения запроса подключения, маршрутизатор NAT преобразовывает

это в следующий доступный IP-адрес реального сервера (например, 10.1.1.2) и затем передает пакет к серверу.

С тех пор статический NAT является двунаправленным в другом направлении, назначение пакета будет преобразовано. При выполнении этой формы NAT мы должны инициировать его путем передачи пакетов TCP. Передача Протокола ICMP не могла бы инициировать преобразование NAT.

Трафик НЕ TCP направлен к первому адресу в пуле.

В отличие от статического внутреннего источника NAT и статический внутренний исходный PAT, маршрутизатор не отвечает на запросы ARP о глобальном адресе, пока тот адрес не назначен на его интерфейс. Поэтому может быть необходимо добавить его к интерфейсу как вторичное устройство. Не возможно перенаправить порты с этим методом трансляции (например, 80 и 1087). Порты должны совпасть.

Шаги

1. Определите пул адресов, содержащих адреса реальных серверов.

ip nat pool NATPOOL 10.1.1.1 10.1.1.3 длины префикса 24 ротации типа

1. Определите access-list, который разрешает адрес виртуального сервера.

хост 172.16.2.3 разрешения access-list 1

1. Включите динамическое преобразование внутренних адресов назначения (DA).

список ip nat inside destination <пул *name> ACL <Имя пула>*

список 1 ip nat inside destination объединяет NATPOOL

1. Теперь определите NAT внутри и внешние интерфейсы.

IP-адреса 10.1.1.1, 10.1.1.2 и 10.1.1.3 будут теперь розданы ротационной формой, когда кто-то попытается обратиться к IP 172.16.1.3

Можно проверить это путем инициирования несколько TCP - сеансов от внешних хостов до виртуального IP. Выходные данные Трансляции/show ip nat translation Debug IP NAT могут использоваться для проверки.

Проверка

Ограничения

1. Это не может обнаружить, отказывает ли внутренний сервер в группе. Это означает, что Cisco IOS всегда будет передавать трафик к серверам в группе, независимо от их рабочего состояния.
2. Это не может определить действующие нагрузки внутренних серверов, таким образом, это не может выполнить распределение нагрузки эффективно.